TM:NDB
F.#2016R00943

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

17M109

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE NAME JAY MILLER AND ICLOUD SUBSCRIBER NUMBERS 10306712515 AND 10306740923 THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

**APPLICATION FOR A SEARCH WARRANT**

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Stacy Shahrani, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the name Jay Miller and iCloud subscriber numbers 10306712515 and 10306740923 that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since December 2008. My training and experience has included investigating crimes

facilitated by the use of electronic communication devices, including smartphones, and cloud-storage and cloud computing services, including iCloud.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1591 (sex trafficking of children) and 1952 (promotion of a prostitution business) committed by MICHAEL MILLER, also known as "Jason m," "mikegmiller" and "Jay," and LATRELL KING, also known as "Lala Banks," "Lala Miller," and "Lartrell King," as described in Attachment B.

## PROBABLE CAUSE

5. On or about August 14, 2016, defendants MICHAEL ANDRES MILLER, also known as "Jason m," "mikegmiller," and "Jay," LATRELL KING, also known as "Lala Banks," "Lala Miller," and "Lartrell King," and SHAREKUL ISLAM were arrested by officers of the Swatara Township Police Department in Harrisburg, Pennsylvania, in connection with the promotion of prostitution of a minor (the "Victim"). Police reports concerning the arrest provide, in sum and substance and part, that ISLAM worked for MILLER and KING as a driver who was paid to drive the Victim to and from hotels where she would engage in prostitution. The Swatara Township police investigation also revealed

that these transactions or "dates" were arranged by MILLER and/or KING, and that MILLER, KING and ISLAM, together with the Victim, had driven to Pennsylvania from New York for the purpose of having the Victim engage in prostitution.

6. Leading up to the defendants' arrest, at approximately 1:45 a.m. on August 14, 2016, a police officer on foot patrol detected the odor of marijuana coming from room 165 of the Howard Johnson Inn located at 473 Eisenhower Boulevard, Swatara Township, Dauphin County Pennsylvania. The officer requested additional police support and went to the front desk. The desk clerk informed the officer that the room was rented to an individual who provided an address in Astoria, Queens. The officer then returned to room 165, by which time additional officers were present. Officers observed ISLAM sitting in a car displaying a New York registration that was in close proximity to room 165, and saw the Victim get into the vehicle. Believing ISLAM and the Victim may be involved in the investigation of room 165, officers approached the vehicle and engaged ISLAM in conversation.

7. Officers detected the odor of marijuana coming from the vehicle and noticed that ISLAM was shaking. When asked about his shaking, ISLAM stated that he was nervous. Officers also observed the Victim, who was dressed in clothing that was tight and exposed her midsection. She also appeared nervous. During this interaction, ISLAM received text messages on his cellular telephone ("Islam's Phone"), and viewed them in such a way that the officer with whom he was speaking could also see them. The messages appeared to be from ISLAM's mother and asked what he was doing, where he was and if he was alright.

8. After ISLAM gave officers confusing and conflicting answers to questions concerning why he was at the hotel, who he was with, and where he was going, an officer asked ISLAM if he would step out of the vehicle to speak. ISLAM agreed and walked a short distance from the vehicle with the officer. The officer asked ISLAM about prostitution, and ISLAM laughed and turned away from the officer. ISLAM denied having anything to do with prostitution. The officer asked if he could look at Islam's Phone. After hesitating, ISLAM told the officer that he had nothing to hide and granted permission for the officer to retrieve Islam's Phone from the vehicle. ISLAM provided the officer with the passcode to Islam's Phone and allowed him to look through the device. Officers also discovered $200 in cash on the floor of the passenger seat, where the Victim was seated.

9. While ISLAM spoke with the officer outside the vehicle, another officer spoke with the Victim and determined that the Victim was 14 years old.

10. MILLER and KING were subsequently arrested in a hotel room at another hotel in East Pennsboro Township, Cumberland County Pennsylvania. The police recovered KING's cellular telephone ("King's Phone") incident to KING's arrest. KING subsequently admitted to law enforcement that the device was hers.

11. Later, ISLAM provided written consent to agents to search Islam's Phone. The messages on Islam's Phone included messages from "Jays Wifee Lala" at 347-944-8504, later confirmed to be KING using her cellular telephone, King's Phone. Those messages contained communications concerning locations, which, as ISLAM later explained, were the locations where he was to pick up and drive the Victim to engage in prostitution. Among the messages from "Jays Wifee Lala" was one that was sent soon after ISLAM had picked the

Victim up in New York, prior to driving to Pennsylvania, asking, about the Victim, "[i]s she fat?" Another message from "Jays Wifee Lala" instructs ISLAM to "[c]ome to the hotel" and provides an address.

12. A review of the subpoena return for King's Phone revealed that the device is connected to two iCloud subscribers: iCloud subscriber number 10306712515, associated with Apple ID mikegmiller@gmail.com, and 10306740923, associated with Apple ID money0mike@aol.com. Both iCloud subscribers are registered under the name "Jay Miller."

13. ISLAM confirmed to law enforcement that MILLER uses the alias "Jay."

14. Both iCloud email handles, "mikegmiller" and "money0mike," are believed to have been used by MILLER to facilitate the sex trafficking of minors. In or about early 2016, MILLER, using the "mikegmiller" handle, communicated with and recruited a known minor victim in Queens, New York, via the messaging application "Kik." Additionally, a review of subpoena returns from Backpage.com, a website used to advertise prostitution for, among others, minor victims of MILLER and KING's sex trafficking conspiracy, revealed that Backpage ads providing contact telephones associated with MILLER and/or KING were created by a user who registered with the email account "money0mike@aol.com."

15. Based on this information, and based on the manner in which iCloud generates and stores information as set forth below, I submit that there is probable cause to search the iCloud account(s) associated with Jay Miller and iCloud subscriber numbers 10306712515 and 10306740923 for the information set forth in Attachment B, including subscriber/profile information, SMS, MMS and "iMessage" text and multimedia messages, voicemail, email transmission information, subject headings, to/from information, folders and email content (including all of the foregoing for deleted messages) relating to the sex trafficking of minors.

16. In addition, based on my training and experience, I am aware that backed up data exists in a user's iCloud account that may have been deleted from that user's smartphone, and therefore, information associated with an iCloud account may reveal deleted content.

## INFORMATION REGARDING APPLE ID AND iCLOUD[1]

17. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

19. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

20. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as AOL, AIM, Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

21. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the IP address used to register and access the account, and other log files that reflect usage of the account.

22. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

23. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play

content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

24. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

25. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

26. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including the sex trafficking of minors, as these media are used to communicate and facilitate the offenses.

27. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement, something there is already evidence of here).

29. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

30. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information will likely constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

## INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrant.

33. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Stacy Shahrani
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on February 3, 2017

S/ Steven L. Tiscione
HON. STEVEN L. TISCIONE
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## Property To Be Searched

This warrant applies to information associated with the name Jay Miller and iCloud subscriber numbers 10306712515 and 10306740923 that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014.

# ATTACHMENT B

## Particular Things To Be Seized

### I. Information To Be Disclosed By Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

## II. Information To Be Seized By The Government

All information described above in Section I, that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1591 (sex trafficking of children) and 1952 (promotion of a prostitution business) involving MICHAEL MILLER, also known as "Jason m," "mikegmiller" and "Jay," and LATRELL KING, also known as "Lala Banks," "Lala Miller," and "Lartrell King," during the period from December 1, 2015 through the present, including, for the account(s) listed in Attachment A, information pertaining to the following matters:

a. Sex trafficking, prostitution and escorting including advertising, recruiting, logistics, pricing and scheduling;

b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

e. Evidence indicating the subscriber's state of mind, including any evidence of deletion of content; and

f. Evidence, including communications, that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature